CRYPTOSUDO

Blockchain Developing & Education Ecosystem

Whitepaper v.1.0

TABLE OF CONTENTS

INTRODUCTION TO CRYPTOCURRENCY

CHAPTER 1

1.1 BITCOIN

In 2009, Satoshi Nakamoto released Bitcoin: A peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.
(Satoshi Nakamoto | Bitcoin: A Peer-to-Peer Electronic Cash System | 2009)

1.2 THE BLOCKS

Transaction data is permanently recorded in files called blocks. They can be thought of as the individual pages of a city recorder's record book (where changes to title to real estate are recorded) or a stock transaction ledger. Blocks are organized into a linear sequence over time .

New transactions are constantly being processed by miners into new blocks which are added to the end of the chain. As blocks are buried deeper and deeper into the blockchain they become harder and harder to change or remove, this gives rise of Bitcoin's Irreversible Transactions.
(https://en.bitcoin.it/wiki/Block)

1.3 THE BLOCKCHAIN

A block chain is a transaction database shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history.

Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known.

Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are what make bitcoins transactions irreversible. The block chain is the main innovation of Bitcoin.
(https://en.bitcoin.it/wiki/Block_chain)

1.4 PROOF OF WORK

In fact, PoW idea was originally published by Cynthia Dwork and Moni Naor back in 1993, but the term “proof of work” was coined by Markus Jakobsson and Ari Juels in a document published in 1999.

Either way, Proof of work is maybe the biggest idea behind Bitcoin white paper, because it allows less secure and distributed consensus. PoW is a requirement to define an expensive computer calculation, also called mining, that needs to be performed in order to create a new group of unsecure transactions (called block) on a distributed ledger called blockchain.

1.5 PROOF OF STAKE

The idea of proof of stake algorithm was suggested on the bitcointalk forum back in 2011. The first digital currency to use this method was released in 2012 – Peercoin, together with ShadowCash, Nxt, BlackCoin, NuShares/NuBits, Qora and Nav Coin.

Unlike the proof-of-work, where the algorithm rewards miners who solve mathematical problems with the goal of validating transactions and creating new blocks, with the proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.

1.6 MASTERNODES

Masternodes are full nodes, just like in the Bitcoin network, except they must provide a level of service to the network and have a bond of collateral to participate. The collateral is never forfeit and is safe while the masternode is operating.

This permits masternode operators to provide a service to the network, earn payment for their services and reduce the volatility of the currency. To run a masternode, the operator must demonstrate control over 1,000 DASH. When active, masternodes provide services to clients on the network, and in return receive regular payment from the block reward.
(Dash Whitepaper | Dash: A Payments-Focused Cryptocurrency)

1.7 DARK GRAVITY WAVE 3.0

DGW or Dark Gravity Wave is an open source difficulty-adjusting algorithm for Bitcoin-based cryptocurrencies that was first used in Dash and has since appeared in other digital currencies. DGW was authored by Evan Duffield, the developer and creator of Dash, as a response to a time-warp exploit found in Kimoto's Gravity Well.

In concept, DGW is similar to the Kimoto Gravity Well, adjusting the difficulty levels every block (instead of every 2016 blocks like Bitcoin) based on statistical data from recently found blocks. This makes it possible to issue blocks with relatively consistent times, even if the hashing power experiences high fluctuations, without suffering from the time-warp exploit.
(https://docs.dash.org/en/latest/introduction/features.html#dark-gravity-wave)

1.8 HASH ALGORITHM | X16S (Shuffle)

X16R is a hashing algorithm, which is based on the classic X11. It uses sixteen chained hashing algorithms in an effort to thwart the move to ASIC mining. X16R algorithm has: BLAKE, BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, Echo, Hamsi, Fugue, Shabal, Whirlpool, Loselose, Djb2.
(https://en.bitcoinwiki.org/wiki/X16R)

Just like X16R; **X16S** also has the same 16 sub-algorithms. Instead of randomizing the algorithm X16S shuffles the list to call the sixteen sub-algorithms. This by preserving the randomness it provides consistency in hash rates and power consumption.

INTRODUCING CRYPTOSUDO

CHAPTER 2

2.1 GENERAL DEFINITION

CryptoSudo is the developing and education ecosystem on the basis of Blockchain Technology.

Why do we care so much about Blockchain Technology? Because:

Unlike classic database logic, the Blockchain not collected in a single center or not managed by a specific person. On the contrary, it can be stored on many computers at the same time, and anyone who wants can have a copy of this Blokchain.

With decentralized storage of data; Increases reliability of data storage and processing. All information can be recovered even when a large error occurs.

Blockchain Technology significantly simplifies operations like insurance, banking, deed, law, obligations and property rights records and follow-up of supply chains etc.

Ensures the management of agreements without the need for third parties. Secures the sharing of documents with counterparts and saving time and cost.

Because of the Bitcoin seen by many people only as an investment tool, this technology, unfortunately is often ignored. Our base goal is to make this technology more understandable and create an effective community that will contribute to its development.

We believe that the developers are critical value to Blockchain Technology. Our another goal is to bring new developers to this sector and help existing developers do their jobs well.

We will introduce an online and free training platform about the cryptography and software languages which are basis of this technology. And we will spread this platform to masses.

The community will ask questions to developers within the discussion forum. The members will have the opportunity to improve themselves with short video lessons to be published on Education Platform.

We know how effective the interaction and cooperation to develop creativity and learning in the education. Our ecosystem will be a central development and education platform for Blockchain Technology, supported by SUDO crypto currency.

With CryptoSudo we do not aim to create new patterns. On the contrary, we intend to create a new and creative way beyond the existing patterns. Our primary goal is to become an ecosystem where ideas exchange and constructive criticism are blended with free and open source contents.

In a disciplined and orderly system, we invite everyone to join us and share their ideas with us for an ever-evolving and strengthening formation.

2.2 BASIC GOALS AND PRINCIPLES

- To bring Blockchain Developers together. Increasing cooperation and solidarity.
- To establish management and audit boards with trained and experienced members within the community.
- To produce open source projects and to prepare free educational contents.
- To organize seminar activities to inform the community members about the innovations.
- To guide such as standards, terminology, education, legal regulations, working conditions about Blockchain.
- Create certificates and distribute them to eligible members for free
- To provide technical and scientific advice, to prepare reports, to create cooperation opportunities and to exchange information between members
- Preparing recommendations for the development of Blockchain Technology. To convey these proposals to the relevant institutions and to reflect the results to the public
- To create a documentation center for Blockchain Technology

2.3 BASIC FEATURES OF EDUCATIONAL CONTENTS

- Contents will be based on Blockchain Technology, Cryptography and Software Languages
- Will be published it completely free
- Content producers will be selected and supervised by a board to be formed
- The basic language of instruction will be English and subtitles will be prepared for other languages
- Content priorities and key topics will be determined based on the exchange of ideas and voting within the community

SUDO | CRYPTOCURRENCY PARAMETERS

CHAPTER 3

3.1 SUDO SPECIFICATIONS

SPECIFICATIONS	DESCRIPTIONS
Ticker	SUDO
Total Supply	300.000.000 SUDO *(Three Hundred Million)*
Hash Algorithm	X16S (Shuffle)
Difficulty Algorithm	Dark Gravity Wave v3.0
RPC Port | Mainnet	3935
P2P Port | Mainnet	11919
RPC Port | Testnet	3934
P2P Port | Testnet	11920
Block Time	180 seconds
Block Size	2MB
Block Reward	30 SUDO *(Thirty)*
Maturity	15 Blocks
Send Confirmation	6 Blocks
Masternode Collateral	50.000 SUDO *(Fifty Thousand)*
Masternode Confirmation	15 Blocks
Masternode Reward	60% of Block Reward
PoW Reward	40% of Block Reward
Premine	2% of Total Supply
Protocol Support	IPV4, IPV6, TOR

3.2 BLOCK REWARD SYSTEM

The reward systems contribute to the creation and confirmation of the Blockchain and each new block distributes the reward among those who perform jobs.

First 7200 blocks, reward is, 1 SUDO.
Between 7200 & 8640 blocks, reward is, 30 SUDO.
Between 8640 & 23040 blocks, reward is, 9 SUDO.
Between 23040 & 80640 blocks, reward is, 90 SUDO.
Between 80640 & 138240 blocks, reward is, 75 SUDO.
Between 138240 & 195840 blocks, reward is, 60 SUDO.
Between 195840 & 282240 blocks, reward is, 45 SUDO.
After 282240. block, reward is, 30 SUDO.

Masternode block rewards will begin after block number 8640.

The number of SUDO generated per block is set to decrease geometrically, with a 5% reduction every 1.752.000 blocks, or approximately ten years.

3.3 STATIC RETURN FOR MASTERNODE INVESTORS

Powerful masternode network adds a second tier of computing decentralization. This tear can perform any mathematical or financial task that the community implements.

The masternode network adds two features:

Instand Send: Perform instant transaction that are irreversible and permanent.
Private Send: Improved privacy with automated mixing and chaining.

The SUDO block reward is split such that 60% of rewards are allocated to Masternodes, 40% of rewards are allocated to PoW Miners. Masternode rewards fluctuate based on the current number of masternodes.

To calculate daily masternode payouts formula:

(n/t) * r * b *.60

***n** : Number of Masternode Owned*
***t** : Total Active Masternodes*
***r** : Current Block reward*
***b** : Blocks per a Day*

ACKNOWLEDGMENTS

CHAPTER 4

CryptoSudo would not be possible without the previous works of the Bitcoin, Dash, Ravencoin and Pigeoncoin teams. Open source software and its contributors are constantly paving the way toward new and exciting innovations.

We are excited to belong to an open source community and appreciate the opportunity to contribute to this growing technological field. When knowledge are free to build upon, society as a whole benefits. We are grateful to our predecessors for the opportunity to contribute to this blockchain revolution.

SUDO | LEGAL NOTICES

CHAPTER 5

Before using any cryptocurrency, it is important to consider the nature, complexity and risk.
We strongly suggest seeking advice from your own financial, investment, tax, or legal adviser.

Cryptocurrency investments are inherently high risk. Do not invest more than you can afford to lose.
It is important not to use coins without taking into account the possible loss, since the type of change in these currencies is highly volatile.

REFERENCES

CHAPTER 6

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system
https://bitcoin.org/bitcoin.pdf

Bitcoin Wiki Pages
https://en.bitcoin.it/wiki/Main_Page
https://en.bitcoinwiki.org/wiki/Main_Page

Dash Whitepaper
https://dashpay.atlassian.net/wiki/spaces/DOC/pages/5472261/Whitepaper

Masternode Features
https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend
https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend

Dash Features
https://docs.dash.org/en/latest/introduction/features.html